

BOX PATENT APPLICATION  
Attorney Docket No. 24929

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Kenjiro UEDA, et al.

Serial No. Not Yet Assigned

Filed: March 8, 2002

For: **ENCRYPTION METHOD, DECRYPTION METHOD, AND RECORDING  
AND REPRODUCING APPARATUS**

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner of Patents  
Washington, D.C. 20231

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date March 13, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-070011. Applicant also claims as priority date March 13, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-070012. Applicant further claims as priority date October 9, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-311114. Applicant further claims as priority date October 9, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-311117.

jc997 U.S. PTO  
10/092544  
03/08/02

#3  
8-22-03  
JH

Page 2 of 2

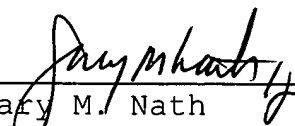
Docket No. 24929

A Certified Copy of the corresponding applications are submitted herewith.

Respectfully submitted,

**NATH & ASSOCIATES PLLC**

Date: March 8, 2002

By:   
Gary M. Nath  
Registration No. 26,965  
Customer No. 20529

**NATH & ASSOCIATES PLLC**  
6<sup>TH</sup> Floor  
1030 15<sup>th</sup> Street, N.W.  
Washington, D.C. 20005  
(202)-775-8383  
GMN/lis (Priority)

jc997 U.S. PTO  
10/092544  
03/08/02

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 13, 2001

Application Number: Patent Application No. 2001-070011

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

December 28, 2001

Commissioner,  
Japan Patent Office

Kozo Oikawa

Number of Certification: 2001-3112879

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

jc997 U.S. PTO  
10/092544  
03/08/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 3月13日

出 願 番 号

Application Number:

特願2001-070011

出 願 人

Applicant(s):

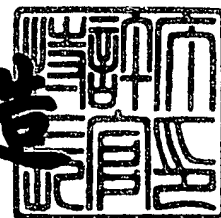
日本ビクター株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年12月28日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3112879

【書類名】 特許願

【整理番号】 413000021

【提出日】 平成13年 3月13日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 20/10

【発明者】

    【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

    【氏名】 上田 健二郎

【発明者】

    【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

    【氏名】 菅原 隆幸

【発明者】

    【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

    【氏名】 猪羽 渉

【発明者】

    【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

    【氏名】 日暮 誠司

【発明者】

    【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

    【氏名】 黒岩 俊夫

【特許出願人】

    【識別番号】 000004329

    【氏名又は名称】 日本ビクター株式会社

    【代表者】 守隨 武雄

【電話番号】 045-450-2423

【手数料の表示】

【予納台帳番号】 003654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書  
【発明の名称】 暗号化方法  
【特許請求の範囲】

【請求項 1】

複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、

所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法。

【請求項 2】

再生順序のある複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、

所定の単位ブロックを暗号化するための暗号鍵のシードは、前記再生順序にて前記所定の単位ブロックより前の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロックより前の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法。

【請求項 3】

前記暗号鍵のシードが少なくとも 2 回以上連鎖していること特徴とする請求項 2 に記載の暗号化方法。

【請求項 4】

前記連鎖が所定の回数でリセットされることを特徴とする請求項 3 に記載の暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、視聴制限のあるコンテンツを暗号化する際の暗号化方法に関するものである。

【0002】

## 【従来の技術】

従来、映像や音声等のコンテンツは、ビデオテープやオーディオテープ等のテープ状記録媒体に記録されたり、CDやDVD等のディスク状記録媒体に記録されたりしているが、これらの媒体に記録されたコンテンツをダビング等の行為によって不正にコピーされることが問題となっていた。

## 【0003】

また、映像や音声等のコンテンツを記録する際にデジタル方式が採用されるようになり、上述した媒体への記録の他にデータ配信などによってもコンテンツが配布されるようになり、不正なコピーの防止はより重要になってきている。

## 【0004】

次に、デジタルコンテンツデータに対するコピーの制限方法について説明する。近年、上述したように映像や音声のデジタル配信が普及してきたことにより、コンテンツの配信を行うコンテンツプロバイダによってデジタルコンテンツデータに「コピー禁止」や「一回コピー可」等の視聴制限をかけていた。このようなデジタルコンテンツデータでは、コンテンツの中にコピーガード信号を挿入することにより、コピーしようとしたときに、コピーした側のコンテンツの映像が乱れるといった効果をもたらしていた。

## 【0005】

このような方法を採用したコピーガードの代表的なものとしてマクロビジョン方式（擬似シンクパルス方式、カラーストライプ方式）と呼ばれるものがある。これは、「コピー禁止」の制限がかかったコンテンツのアナログ信号の特定部分に一定の信号を組み込むことにより、このコンテンツを録画しても、録画機器が特定部分に組み込んだ信号を認識しながら録画するため、コピー後の画面を再生すると前述した信号の影響で画面が鑑賞に堪えないものになってしまう方法である。また、この方式のコピーガードを採用したコンテンツをデジタル録画機器で録画しようとしても、録画機器がこの信号を認識して録画ができない仕組みとなっている。なお、デジタル放送のPPV（Pay Per View）番組にはこの方式が採用されている。

## 【0006】



しかしながら、この方式のコピーガードでは画面を乱す信号を除去するだけで正常な状態でコピーできるため、このコピーガードを回避するための機器が市販されるようなことが行われてきた。

## 【 0 0 0 7 】

また、「一回コピー可」の制限がかかったコンテンツについてはコピー世代の管理をすることによって規定回数以上のコピーを防止してきた。この方法の代表的なものとしては、CGMS (Copy Generation Management System) と呼ばれるものがある。これは、コンテンツのデジタル信号の特定の箇所に特定のデジタル信号 (1. コピー不可, 2. コピー一代のみ可, 3. コピー無制限の三通り) を組み込み、この信号をデジタル録画機器が識別することにより、そのコンテンツに組み込まれる特定のデジタル信号が指示するようにコピーを制限する方法である。なお、MD (ミニディスク) のコピー世代管理にもCGMS方式が採用されている。

## 【 0 0 0 8 】

しかしながら、CGMS方式もコピー世代に関するフラグを「コピー不可」のものから「コピー可能」のものに書き換えることによってコピーガードを解除することができた。

## 【 0 0 0 9 】

このようなことを踏まえて、DVDではデジタルコンテンツデータ自体に暗号をかけて媒体に記録するようにした。従って、データをそのまま取り出そうとしても暗号化がかかっているコンテンツを取り出すことになり、しかも、暗号鍵を取り出すことは困難であるので、実際に暗号化がかかっていないデジタル信号をコピーするのは難しくなった。

## 【 0 0 1 0 】

このような暗号化の方式の一つであるDES (Data Encryption Standard) について説明する。DESは平文(原文)、暗号文、暗号鍵共に64ビットのサイズを持つブロック暗号である。ただし、暗号鍵は64ビットのうち8ビットをパリティに使用しているため、実質的な暗号鍵の長さは56ビットである。

## 【 0 0 1 1 】

DESの基本構成を図1に示す。平文の隣り合った各ビットがほぼ32ビット離れるようにビットの入れ替えが行われた後、16段の同一の変換が繰り返し適用される。各段では、前段から入力される上位32ビットの $L_{n-1}$ と下位32ビットの $R_{n-1}$ をそれぞれひとまとまりとし、鍵生成部から入力される48ビットの鍵 $K_n$ を用いて、それらを $L_n$ と $R_n$ に変換して次段に出力する。そして、16段目の出力の $L_{16}$ と $R_{16}$ とを入れ替えた後、 $IP^{-1}$ により各ビットを置換することで暗号文が出力される。一方、鍵は選択置換PC-1により8ビットのパリティビットが取り除かれると共に、残りの56ビットの入れ替えが行われる。

## 【0012】

その後、上位28ビットの $C_n$ と下位28ビットの $D_n$ をそれぞれひとまとまりとしてシフトを16段繰り返しながら、各段毎に鍵 $K_n$ を作成する。図1に示したDESの基本単位である16段の変換部は各段共に図2に示す構造となっており、前段からの入力( $L_{n-1}$ ,  $R_{n-1}$ )と次段の出力( $L_n$ ,  $R_n$ )は次の関係を満たす。

$$L = R_{n-1}, \quad R_n = L_{n-1} \text{ XOR } f(R_{n-1}, K_n)$$

ここでは、XORは排他的論理和を示しており、関数 $f(R_{n-1}, K_n)$ は、更に図3に示す構造を有している。

## 【0013】

$f$  関数への入力 $R_{n-1}$ は32ビットからなるが、拡大置換Eにより、48ビットに拡大される。次に、その48ビットと $K_n$ とをビット単位で排他的論理和を取った後、6ビット単位の8個に分割され、それぞれが $S_1 \sim S_8$ のSボックスに入力される。各Sボックスでは6ビットの入力が4ビットの出力に非線形変換される。最後に、その出力の4ビットを8個合わせた32ビットが、置換Pによりビット位置が入れ替えられ、 $f(R_{n-1}, K_n)$ の出力となる。

## 【0014】

DESの基本変換である式

$$L_n = R_{n-1}, \quad R_n = L_{n-1} \text{ XOR } f(R_{n-1}, K_n)$$

を解いて、( $L_{n-1}$ ,  $R_{n-1}$ )を( $L_n$ ,  $R_n$ )で表すと次式となる。

$$R_{n-1} = L_n, \quad L_{n-1} = R_n \text{ XOR } f(R_{n-1}, K_n) = R_n \text{ XOR } f(L_n, K_n)$$

)

これによって  $(R_n, L_n)$  から  $(R_{n-1}, L_{n-1})$  を求める操作は、 $(L_{n-1})$  から  $(L_n, R_n)$  を求める操作を同じ構造になっていることが分かる。この性質は、復号を暗号化と同じ変換で行うことができることを意味している。

【 0 0 1 5 】

【発明が解決しようとする課題】

しかしながら、例えばデジタル放送の P P V 番組では「コピー禁止」の制限がかかっているため、そのコンテンツを一回だけ視聴することができるが、視聴者は P P V 番組が放送されている決まった時間帯に見なければいけなかった。このように、「コピー禁止」のコンテンツについては、その著作権者がコンテンツの視聴を一回だけ許可する意図であったとしても、実際には視聴する時間帯を限定してしまうことになっていた。また、「コピー禁止」のコンテンツを記録媒体に記録して一回だけ視聴を許可する場合も、一回コンテンツを視聴したらコンテンツの再生を不可能とする方式が確立されていなかった。更に、これを実現するために、コンテンツを再生しながら見終わった部分のデータを消去するというのは処理が難しく実現が困難であった。例えば、パーソナルコンピュータ等でハードディスク上のデータを削除するのはファイルシステムの F A T を消去しているだけなので、実際にデータを消去しているわけではなかった。

【 0 0 1 6 】

一方、「一回コピー可」のコンテンツは、例えば V T R と H D D (ハードディスクドライブ) とを組み合わせた記録再生装置で記録する場合でも一回どちらかの媒体に記録したらそれ以上の記録は二回目のコピーとなってしまいうためできなかった。従って、一度視聴した後に所望の番組だけを保存用の媒体に改めて記録することはできなかった。このように、「一回コピー可」のコンテンツについては、その著作権者がコンテンツが記録される媒体は一つに限定するという意図であったとしても、実際には一度記録したコンテンツを別の媒体に記録して元の記録媒体の記録部分を消去する、いわゆるコンテンツの移動が許可されていなかった。

【 0 0 1 7 】

また、暗号化に関しても、コンピュータの性能の向上によって暗号鍵を知ることが容易となった。そして、一つのコンテンツに固定の鍵を使用することは、その鍵を知ることができたらそのコンテンツ全てが解読されたことになり、その結果、デジタルコンテンツが違法にコピーされることが予想される。そこで、これを回避するために鍵を時間毎に変化させるという方法がある。これによってコンテンツの一部の暗号化に使用された鍵が知られても、コンテンツ全体が解読されたことにはならず、固定の鍵をしようする場合に比べて安全性は増す。また、復号時に複数の鍵を生成する際に暗号化に使用した鍵を計算するが、その鍵又はその鍵のシードを別に記憶しておく必要があるが、この方法ではその記憶量が複数の鍵の個数に比例して大きくなるという欠点がある。ここで「鍵のシード」とは鍵の生成の元になる情報を表している。

## 【 0 0 1 8 】

更に、暗号化に関しては特開平 9 - 1 0 7 5 3 6 号公報に記載されているように、ブロック連鎖法における暗号化処理として、 $P(1)$  を暗号鍵  $K$  及び初期値  $IV$  に依存させて、暗号化関数  $E_1$  を用いて暗号化し、 $P(i)$  ( $2 \leq i \leq n$ ) は、暗号鍵  $K$  及び  $P(i-1)$  に依存させて、暗号化関数  $E_2$  を用いて順次暗号化し、暗号化されたデータブロック ( $C(1)$ ,  $C(2)$ , ...,  $C(n)$ ) を生成する方法が開示されている。しかしながら、この場合には、暗号鍵  $K$  が固定であり、暗号化の基になるデータが暗号化を行うデータの前のデータであるため、暗号化が解かれる危険性が高いという問題があった。

## 【 0 0 1 9 】

## 【課題を解決するための手段】

上述した課題を解決するために、複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法を提供する。

## 【 0 0 2 0 】

また、再生順序のある複数の単位ブロックが連続した情報を単位ブロック毎に

暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記再生順序にて前記所定の単位ブロックより前の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロックより前の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法を提供する。

## 【 0 0 2 1 】

更に、前記暗号鍵のシードが少なくとも 2 回以上連鎖していること特徴とする請求項 2 に記載の暗号化方法を提供する。

## 【 0 0 2 2 】

また、前記連鎖が所定の回数でリセットされることを特徴とする請求項 3 に記載の暗号化方法を提供する。

## 【 0 0 2 3 】

## 【発明の実施の形態】

以下、本発明に係る暗号化方法の一実施例について図面を参照して説明する。デジタルコンテンツデータが放送局から送られてくる A V データであり、「コピー禁止」である場合、放送が行われた時間帯以降の任意の時間にその番組を一回だけ視聴できる記録再生装置としてハードディスクレコーダーを例に説明する。

## 【 0 0 2 4 】

本実施例では、「コピー禁止」のコンテンツについて、一回のみ視聴可能とすることでこのようなハードディスクレコーダーを実現している。ハードディスクには M P E G (Motion Picture Expert Group) のトランスポートストリーム (T S) を記録する。なお、暗号化／復号化には D E S を使用する。

## 【 0 0 2 5 】

図 4 は本発明に係る暗号化方法を適用した暗号化部を内蔵したハードディスクレコーダーの記録部を示す図である。チューナー 1 や外部信号入力部 2 によって M P E G の T S が入力されて、スイッチ回路部 3 へ送られる。ここでユーザーインターフェース 2 0 0 によって出された指示に従って、チューナー 1 又は外部信号入力部 2 から記録信号処理部 4 に信号が送られる。記録信号処理部 4 に送られた信号に対してそこでタイムコード、絶対トラック番号などが生成される。その

後、信号は暗号化部 5 に送られてデータの暗号化が行われる。そして、記録部 6 においてディスク 1 0 0 に記録される。なお、ディスク 1 0 0 には、映像信号、音声信号の他にタイムコードなどが例えばサブコードエリアに記録される。

## 【 0 0 2 6 】

また、図 5 は本発明に係る暗号化方法によって暗号化された信号を復号化する復号化装置を内蔵したハードディスクレコーダーの再生部を示す図である。まず、再生部 1 0 によってディスク 1 0 0 の信号を読み取り、読み取った信号は復号化部 9 に送られる。そこでデータの復号化が行われた後、再生信号処理部 8 に送られ、エラー訂正等が行われた後、外部信号出力部 7 を介してモニタ 3 0 0 に出力される。

## 【 0 0 2 7 】

このように図 4 及び図 5 に示す構成のハードディスクレコーダーにおいて、「コピー禁止」のデジタルコンテンツデータを記録する場合には、「コピー禁止」を示す信号を前述した CGMS によって記録する。例えば、デジタル放送では、TS に digital copy control descriptor という記述子があり、更にその中に digital recording control data (デジタルコピー制御情報) という 2 ビットのフィールドがある。そのフィールドの中に例えば「コピー可」= 0 0、「一回コピー可」= 1 0、「コピー禁止」= 1 1 というように記述される。入力された信号に対して、ハードディスクレコーダーが「1 1」という 2 ビットを検知すると、同一コンテンツでは一定の  $Const_i$  を初期ベクトル生成関数  $h_i$  の入力として初期値  $IV = h_i (Const_i)$  を計算する。

## 【 0 0 2 8 】

初期値  $IV$  は、入力されたコンテンツの最初の単位ブロックを暗号化する際の鍵のシードとなるものである。従って初期値  $IV$  が簡単に知られてしまうと暗号化されたコンテンツが解読される恐れがあるので、初期値  $IV$  はハードディスク外の解析が困難な媒体に記録する。媒体としては、例えば、取り外しが困難なフラッシュメモリー等を使用する。この場合、単位ブロックを 1 8 4 バイトとして考えると、初期値  $IV$  を鍵生成関数  $g$  の入力として鍵  $K_1 = g (IV, Const)$  を計算する。以後、 $K_i$  は、 $i$  番目のブロックを暗号化／復号化する際に使

う鍵を表すものとする。また、Const は鍵生成の元になるその他の情報を表すものとする。ここで、Const の情報が同一コンテンツ内で時間と共に変化するものと仮定すると、Const の情報を記憶しておかなければならない。また、それらの情報が時間と共に変化するものである場合、変化した全ての情報を記憶しておくための大容量のフラッシュメモリーを使用しなければならなくなるので、Const は例えばハードディスク固有の ID など同一のコンテンツ内で一定のパラメータからなるものとする。なお、暗号化／復号化には DES を使用しているので、鍵  $K_i$  が 56 ビットである必要がある。よって、初期値 IV と Const とのビット数の合計が 56 ビット以上になる方が好ましい。なぜならば、鍵生成関数  $g$  が 1 対 1 関数であると鍵  $K_i$  から初期値 IV や Const が推測し易くなるからである。従って、鍵生成関数  $g$  が  $n$  ( $n \geq 2$ ) 対 1 関数となるようにする。

## 【 0 0 2 9 】

次に図 6 を用いて本発明に係る暗号化方法について説明する。1 TS パケットの 188 バイトのうち、ヘッダの 4 バイトを除いた単位ブロックの 184 バイトという値は、AV データが記録されている領域のバイト数である。TS パケット P (1) の AV データである 184 バイトの中に DES の暗号化ブロック 64 ビットが 23 ブロック分ある。そして、この 23 ブロックに対してそれぞれ TS パケット P (1) の暗号化鍵  $K_1$  で暗号化する。なお、暗号化された P (1) は C (1) と記載する。なお、TS パケット P (2), P (3), … に関しても同様の操作を行う。

## 【 0 0 3 0 】

次に、P (2) の暗号化に使用する鍵  $K_2$  の作成方法を説明する。鍵  $K_2 = g(S_1, \text{Const})$  と定義する。ここで、 $S_1$  とは鍵シード生成関数を  $h$  とすると  $S_i = h(P(i))$  で定義されるものとする。すなわち、一つ前の単位ブロックの平文を鍵のシードとする。これによって鍵は 1 単位ブロック毎に可変になり、たとえ一つの鍵が分かっても全ての平文を解読するのは困難である。また、このほかにも鍵のシードを複数用意することによって鍵を可変にする方法があるが、全ての鍵のシードを別に記憶しておく必要があった。しかし、本発明の方法を採

用すると、鍵のシードの可変部分はハードディスク上に記録している暗号文を復号化した平文であるから、解析することも困難で別の領域に記憶しておく必要もない。 $K_3$ 以降も $K_3 = g(S_2, \text{Const})$ ,  $K_4 = g(S_3, \text{Const})$ , ...となる。

## 【0031】

一方、再生するにはフラッシュメモリー上の初期値  $IV$  を読んで鍵  $K_1$  を生成し、 $P(1)$  を暗号化する。その際、 $P(1)$  から  $S_1$  も同時に生成しておく。次に、その  $S_1$  から鍵  $K_2$  を生成し、 $P(2)$  を暗号化する。暗号化と復号化の概略を図7に示す。また、上述した実施例では、一つ前の単位ブロックから暗号鍵のシードを生成していたが、単位ブロックの暗号鍵のシードを過去の一つの単位ブロックから生成しても良く、例えば二つ前の単位ブロックを使用しても良い。

## 【0032】

次に、「コピー禁止」のコンテンツを途中まで再生したときに、一度再生した部分が見られないようにする方法について説明する。図8に示すようにTSパケット  $C(1)$  から  $C(4)$  までは再生するものとする。上述した説明のように、まず初期値  $IV$  を読んで  $C(1)$  から復号化を開始する。そして、 $C(4)$  の復号化を終了した時点で再生を終了する。ここで、次回に  $C(1)$  から  $C(4)$  までのデータを再生できないようにするために、フラッシュメモリーに記録されていた初期値  $IV$  を消去する。これによって  $C(1)$  を復号化するための鍵  $K_1$  を生成することができなくなる。しかし、次回、 $C(5)$  から再生を開始するためには  $C(5)$  を復号するための鍵  $K_5$  のシード  $S_4$  を記録しておかなければならない。従って、再生を開始した時点で初期値  $IV$  をフラッシュメモリーから消去、又は、その後必要な場合はバッファに移動する。そして、再生を終了した時点で  $S_4$  をフラッシュメモリーに記録する。これにより、次回は  $C(1)$  から  $C(4)$  が復号できないことにより再生ができなくなる。一方、フラッシュメモリーに  $S_4$  と共に  $P(5)$  の先頭アドレス等を記録しておくことによって次回から  $C(5)$  以降の再生が可能になる。この例では、 $S_i$  は  $C(i+1)$  の復号化に使用する鍵  $K_{i+1}$  のシードとなっているが、二つの初期値  $IV_1$  と  $IV_2$  とを持つこと



によって  $S_i$  を  $C(i+2)$  の復号化に使用する鍵  $K_{i+2}$  のシードにしても良い。同様に、初期値  $IV$  を 3 つ、4 つ、…と持つことによって、 $S_i$  を 3 つ、4 つ先の単位ブロックを復号化するためのシードとして使用可能である。また、 $K_{i+2}$  のシードを  $S_i$  と  $S_{i+1}$  のように複数にする、すなわち過去の二つ以上の平文を元に鍵を生成しても良い。このように  $S_i$  が  $K_{i+1}$ 、 $S_{i+1}$  が  $K_{i+2}$ 、…のシードになっていることを以後、「連鎖している」と呼ぶこととする。

## 【0033】

元々、「コピー禁止」のコンテンツは放送時に一度だけ視聴することができるという趣旨で放送されているものである。従って、一度再生した部分を巻戻して視聴するのは著作権者の意図に反する可能性が高いので許可されないことがある。しかし、現行の「コピー禁止」のコンテンツは巻戻して視聴することができないのは当然であるが、途中から視聴することは可能である。よって、「コピー禁止」のコンテンツをハードディスクレコーダーに記録して、早送りのみは許可される可能性はある。そこで、上述した方法で早送りを行うと、ランダムアクセスに優れたハードディスクであるにもかかわらず、必ず  $C(1)$  から復号していかなければならない。従って、コンテンツの後半の方から視聴するようなことがあると、そこまでアクセスするのに非常に時間がかかってしまう。そこで、以下のような構成が考えられる。

## 【0034】

図9にその概略を示す。図中の矢印は矢印の始点にある情報が指している情報を暗号化するための鍵のシードになることを示す。隣ブロックの連鎖をこまめにリセットして、その代わりにリセットがかかった次に  $P(2-1)$  というブロックを設ける。 $P(2-1)$  は、初期値  $IV$  をシードにした鍵で暗号化される。そして、 $P(2-1)$  は  $P(2-2)$  と  $P(3-1)$  の暗号化鍵のシードとなる。このような構成により、例えば  $P(3-4)$  にアクセスしたい場合は、初期値  $IV \rightarrow P(2-1) \rightarrow P(3-1) \rightarrow P(3-2) \rightarrow P(3-3) \rightarrow P(3-4)$  という順序で復号していけば短い時間でアクセスすることが可能となる。このような構成を以後二つの「階層」と呼ぶことにする。そして、 $P(2-1)$ 、 $P(3-1)$ 、 $P(4-1)$ 、…のことを「第2階層」と呼ぶことにする。なお

、上述した実施例では、この階層の数が二つの場合を説明したが、階層の数を三つ以上にしても良い。しかし、階層の数を三つ以上にするとランダムアクセスにかかる時間が短縮されるという利点があるものの、暗号化／復号化の方法が複雑になるという欠点がある。なお、ここからは、第1階層の単位ブロックを暗号化／復号化する鍵のシードを生成する関数を $h_1$ 、第2階層の単位ブロックを暗号化／復号化する鍵のシードを生成する関数を $h_2$ 、…と記述する。また、第2階層の $P(2-1)$ によって生成される鍵 $K_{3-1}$ のシードを $T_{2-1}$ 、 $P(3-1)$ によって生成される鍵 $K_{4-1}$ のシードを $T_{3-1}$ 、…とする。

## 【0035】

次に、複数の階層になっている場合に、コンテンツの一度再生した部分を視聴不可能とする方法について説明する。図10に示すように、TSパケット $C(1-1)$ から $C(2-3)$ までを再生するものとする。再生開始時には、フラッシュメモリーには初期値 $IV$ が記録されている。そして、再生を開始した時点で初期値 $IV$ をフラッシュメモリーから消去、又は、その後必要なときにはバッファに移動して、 $C(2-3)$ まで再生が終了した時点で $T_{2-1}$ と $S_{2-3}$ をフラッシュメモリーに記録する。 $S_{2-3}$ を記録する理由は複数の階層を持たなかったときと同様に $K_{2-4}$ を生成するため、すなわち $C(2-4)$ から再生できるようにするためである。一方、 $C(2-3)$ まで再生を終了して、次回、 $C(4-1)$ から再生したい場合には、第2階層の $C(4-1)$ にできるだけ速くランダムアクセスするために、 $T_{2-1} \rightarrow C(3-1) \rightarrow C(4-1)$ と進むのが最も速い。従って、ランダムアクセスのために $T_{2-1}$ もフラッシュメモリーに記録している。更に、 $C(2-4)$ からの再生とランダムアクセスが可能になる。

## 【0036】

以上、ハードディスクレコーダーで「コピー禁止」のデジタルコンテンツを記録する際の説明を行ってきた。なお、本実施例ではMPEGのTSパケットのデジタルコンテンツデータに相当する184バイトを単位ブロックのサイズとして取ってきたが、これはアプリケーションに応じてさまざまなサイズを取ることが可能である。図7や図9のような連鎖を一つのコンテンツを通して行った場合、途中でデータを誤って読み取ったり、誤って記録したりすることで正しく再生で

きなくなることがある。この場合、一箇所の誤りがその後も連鎖するために起きるものなので、これを防止するために初期値 I V から始まる連鎖を同一コンテンツ内で複数回リセットするという方法を取ることもできる。例えば図 1 1 に示すように初期値 I V を複数用意することによって連鎖が複数回リセットされることになるので、誤りの伝播を防止することができる。

## 【 0 0 3 7 】

なお、本実施例ではハードディスクレコーダーについてのみ説明してきたが、「コピー禁止」のコンテンツの場合には、光ディスクレコーダーなどでも実現可能であるし、ランダムアクセスができなくなるが、コンテンツを最初から再生する場合にはテープレコーダーでも実現可能である。

## 【 0 0 3 8 】

これまでは「コピー禁止」のコンテンツの場合について説明してきたが、以下、放送局から送られてくるデジタルコンテンツデータが「一回コピー可」である場合に、その番組を一つの別媒体にのみ記録することができる記録再生装置の例としてハードディスクレコーダーとデジタル V T R を組み合わせた記録再生装置について説明する。本発明の実施の形態では、「一回コピー可」のコンテンツについては、一回のみ別媒体に記録可能とすることで、このようなハードディスクレコーダーとデジタル V T R とを組み合わせた記録再生装置を実現した。ハードディスクレコーダーのハードディスクと V T R のビデオテープには M P E G の T S を記録する。そして、暗号化／復号化には D E S を使用する。

## 【 0 0 3 9 】

図 1 2 は、本発明の一実施例であるハードディスクレコーダーとデジタル V T R とを組み合わせた記録再生装置の記録部のブロック図である。同図において、チューナー 1 や外部信号入力部 2 によって M P E G の T S パケットが入力されて、スイッチ回路部 3 に送られる。ここで、ユーザーインターフェース 2 0 0 から出された指示に従って、テープ記録信号処理部 1 2 又はディスク記録信号処理部 1 4 に信号が送られる。テープ記録信号処理部 1 2 に送られた信号に対してはタイムコードや絶対トラック番号等が生成される。その後、テープ記録部 1 3 に送られてテープ 3 0 0 にデジタル記録される。テープ 3 0 0 には映像信号、音声信

号の他にタイムコード、絶対トラック番号等が例えばサブコードエリアに記録される。また、ディスク記録信号処理部14に送られた信号に対してタイムコード等が生成される。その後、ディスク記録部15に送られてディスク100にデジタル記録される。そして、ハードディスクにもテープ同様に映像信号、音声信号の他にタイムコードや絶対トラック番号等が記録される。ディスク再生信号処理部17は、ハードディスクレコーダーにて記録された信号を再生するもので、この再生信号をテープ記録信号処理部12へ送ることによってデータのコピーを行うことができる。

## 【0040】

図13は本発明におけるデジタル信号記録再生装置の再生部のブロック図である。テープ再生時には、テープ再生部19によってテープ300の信号を読み取る。そして、その信号はテープ再生信号処理部18に送られ、そこでエラー訂正等が行われた後、スイッチ回路部3に送られる。また、ディスク再生時には、ディスク再生部21によってディスク100の信号を読み取る。そして、その信号はディスク再生信号処理部20に送られ、そこでエラー訂正等が行われた後、スイッチ回路部3とテープ記録信号処理部17へ送られる。そして、ユーザーインターフェース200によって出された指示に従って、テープ300の再生信号又はディスク100の再生信号を外部信号出力部16を介してモニタ400に出力する。

## 【0041】

次に、図12、図13に示す構成のハードディスクレコーダーとデジタルVTRとを組み合わせた記録再生装置によって、「一回コピー可」のデジタルコンテンツデータを記録する際の説明を行う。「一回コピー可」を示す信号は、「コピー禁止」を示す信号と同様にCGMSによって記録される。例えば、デジタル放送ではTSにdigital copy control descriptorという記述子があり、更にはその中にdigital recording control data (デジタルコピー制御情報) という2ビットのフィールドがある。そのフィールド中で例えば「コピー可」=00、「一回コピー可」=10、「コピー禁止」=11というように記述される。入力された信号に対して、記録再生装置がその「10」という2ビットを検知すると

、同一コンテンツでは一定の $Const_i$ を初期ベクトル生成関数 $h_i$ の入力とし、初期値 $IV = h_i(Const_i)$ として計算する。以下、「コピー禁止」の場合と同様に暗号化を行う。また、「一回コピー可」のコンテンツは「コピー禁止」のコンテンツと異なり、再生に関しては何度行っても良いので、「一回コピー可」のコンテンツは別媒体に記録を行う際に限って鍵を消去することとする。例えば、図8に示すように、ハードディスクに記録された $C(1)$ から $C(4)$ までをテープに記録し始めたらフラッシュメモリーから初期値 $IV$ を消去して、 $C(4)$ までの記録が終了したらシード $S_4$ をフラッシュメモリーに記録する。従って、再生の際には、フラッシュメモリーの初期値 $IV$ は参照をするが、フラッシュメモリーに対しての記録や消去は行わない。

#### 【0042】

また、「コピー禁止」のコンテンツに関しては、元々デジタル放送のPPVのコンテンツが一回のみ視聴可能という意図で放送されているので、途中の単位ブロックから再生した場合、それ以前のデータの再生は許可されず、そのことは考慮する必要がなかった。しかしながら、視聴者が所望の部分だけをコピーしたり、一つのコンテンツを分割して複数のテープにコピーすることもできる。例えば、図14に示すように、 $C(2-3)$ 以降をテープにコピーして、それ以前はハードディスク上で再生できるようにしておくこともできる。その方法としては、まず $C(2-3)$ からテープにコピーを開始し、単位ブロック $C(2-3)$ をコピーし終えた時点で $C(2-3)$ のデータ自体を消去するか $C(2-3)$ のデータを関係のないデータに書き換える。そして、フラッシュメモリーのデータの書き換えは行わない。これによって、コピーが終了すると $C(2-3)$ はデータ自体が存在しないので復号化はできず、同時に $K_{2-4}$ も生成することができない。しかし、初期値 $IV$ と $C(2-1)$ が残っていることにより初期値 $IV \rightarrow C(2-1) \rightarrow C(3-1) \rightarrow$ ということで $C(3-1)$ 以降は復号化が可能になる。従って、これを避けるために $C(3-1)$ までコピーが終了した時点で $C(2-3)$ と同様に $C(3-1)$ も消去する。これで $C(3-2)$ 以降は再生が不可能になる。また、例えば $C(2-3)$ から $C(3-3)$ までコピーする場合は、上述したものを組み合わせることによって $C(2-3)$ と $C(3-1)$ を消して $T$

3-1とS<sub>3-3</sub>とをフラッシュメモリーに記録すれば良い。

【0043】

以上、ハードディスクレコーダーとデジタルVTRとを組み合わせた記録再生装置で「一回コピー可」のデジタルコンテンツを記録する際の説明を行った。なお、ハードディスクレコーダーとデジタルVTRとを組み合わせた記録再生装置についてのみ説明してきたが、「一回コピー可」のコンテンツの場合、ハードディスクドライブ部には光ディスクレコーダー等のランダムアクセスが可能な記録装置であれば置換可能であり、VTR部にはあらゆる記録装置で置換可能である。

【0044】

【発明の効果】

以上、詳述したように、本発明に係る暗号化方法によれば、「コピー禁止」のコンテンツについて、今までは放送時のみしか視聴することができなかったが、視聴者が視聴したい時間にコンテンツを一度のみ視聴することが可能となった。また、「一回コピー可」のコンテンツも、媒体に記録した後で一度限り別の媒体にコピー及び編集することが可能となる。そして、その際にハードディスク上にあるデータのセキュリティに関しては暗号化されることによって保障される。更に、「コピー禁止」のコンテンツに対して途中までコンテンツを見た場合には、それまでの復号化鍵のシードを消去する方法によって途中の地点までの再生を不可能にするという機能も実現可能である。同様に、「一回コピー可」のコンテンツも別の媒体にコピーした部分は再生を不可能とすることができる。また、暗号鍵のシードが所定の単位ブロック以外の平文、もしくは、暗号文であることによって、所望のブロック以降の再生を不可能にするという機能も実現可能である。そして、連鎖する方式を取ることににより、記録しておく鍵のシード情報の容量が非常に少なく済む。

【図面の簡単な説明】

【図1】

DESの基本構成を示す図である。

【図2】

D E S の基本単位である 1 6 段の変換部の構造を示す図である。

【図 3】

D E S で用いられる関数  $f$  の構造を示す図である。

【図 4】

本発明に係る暗号化方法を適用したハードディスクレコーダーの記録部の構成を示すブロック図である。

【図 5】

本発明に係る暗号化方法を適用して記録した信号を再生するハードディスクレコーダーの再生部の構成を示すブロック図である。

【図 6】

本発明に係る暗号化方法における M P E G の T S の構成と暗号化の概略を示す図である。

【図 7】

本発明に係る暗号化方法による暗号化と復号化方法及び復号化装置による復号化を示す図である。

【図 8】

本発明に係る暗号化方法によって暗号化されたコンテンツの再生方法を示す図である。

【図 9】

本発明に係る暗号化方法による暗号化の一例を示す図である。

【図 1 0】

本発明に係る暗号化方法によって暗号化されたコンテンツの別の再生方法を示す図である。

【図 1 1】

本発明に係る暗号化方法による暗号化の別の例を示す図である。

【図 1 2】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタル V T R とを組み合わせた記録再生装置の記録部を示すブロック図である。

【図 1 3】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタルVTRとを組み合わせた記録再生装置の再生部を示すブロック図である。

【図 1 4】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタルVTRとを組み合わせた記録再生装置の再生方法を示す図である。

【符号の説明】

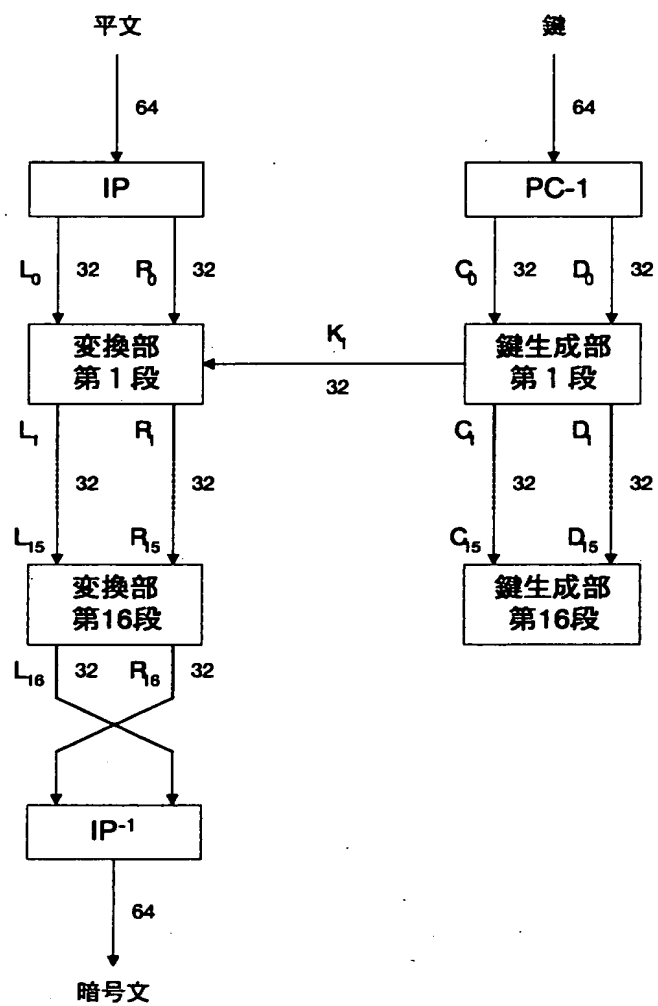
- 1     チューナー
- 2     外部信号入力部
- 3     スイッチ回路部
- 4     記録信号処理部
- 5     暗号化部
- 6     記録部
- 7     外部信号出力部
- 8     再生信号処理部
- 9     復号化部
- 10    再生部



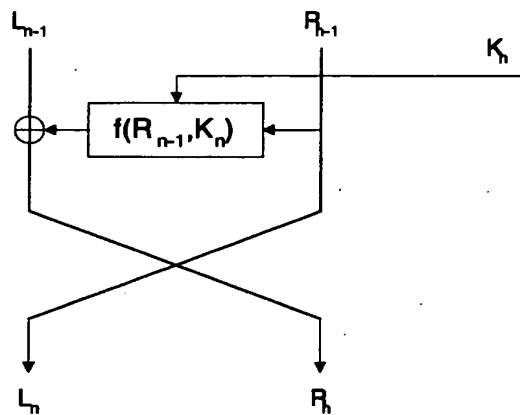
【書類名】

図面

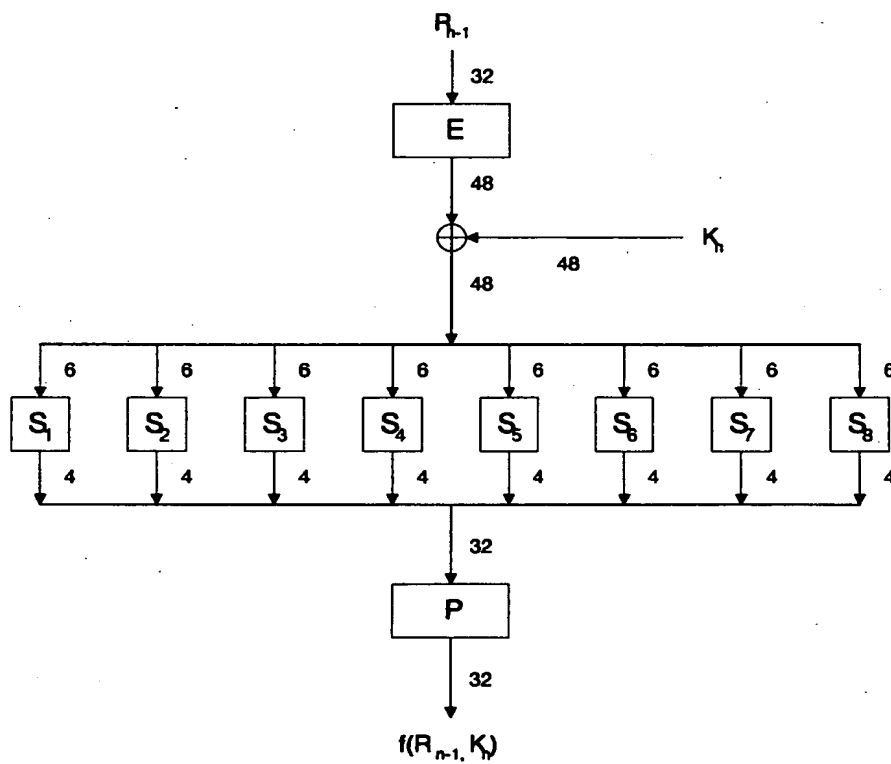
【図1】



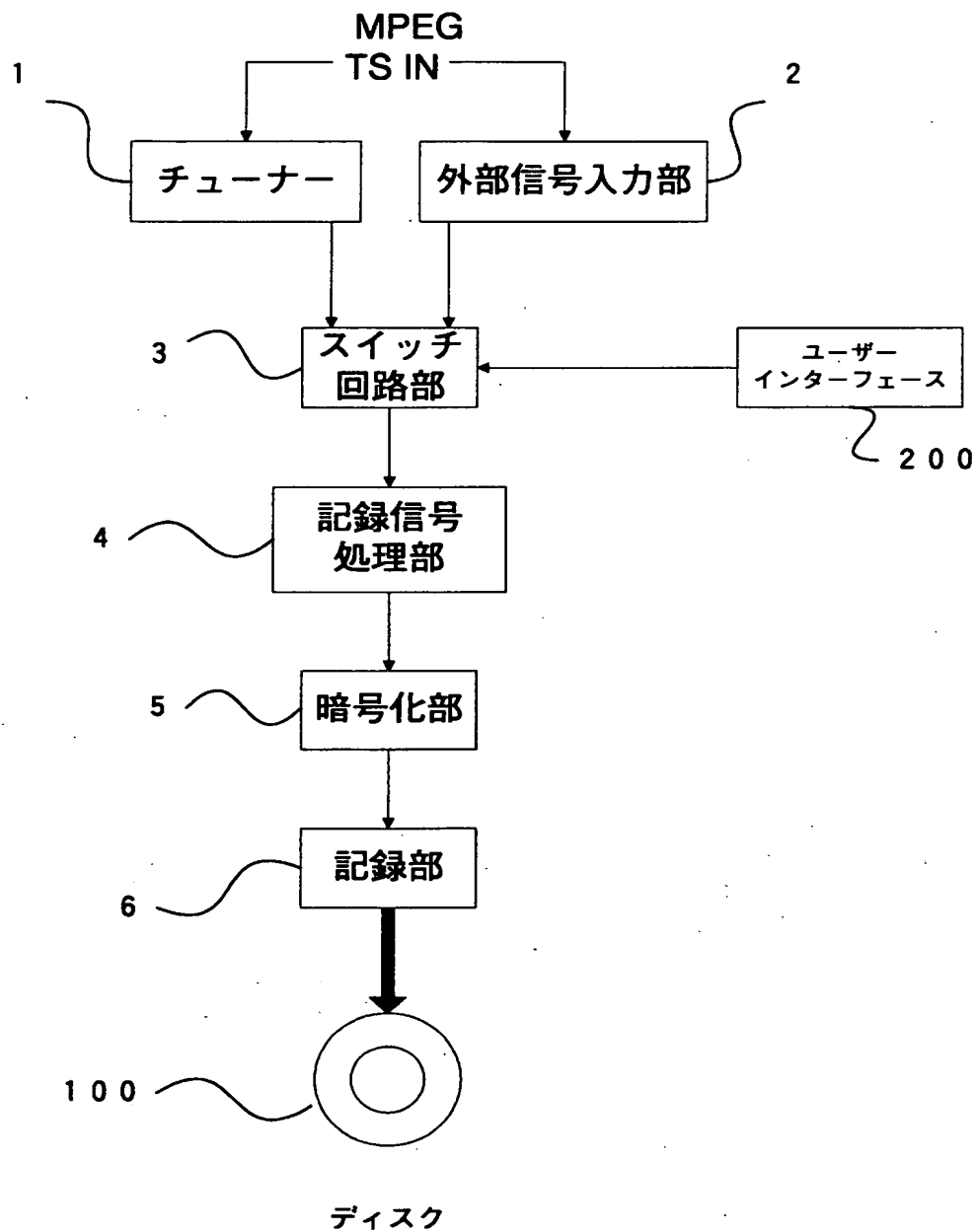
【図 2】



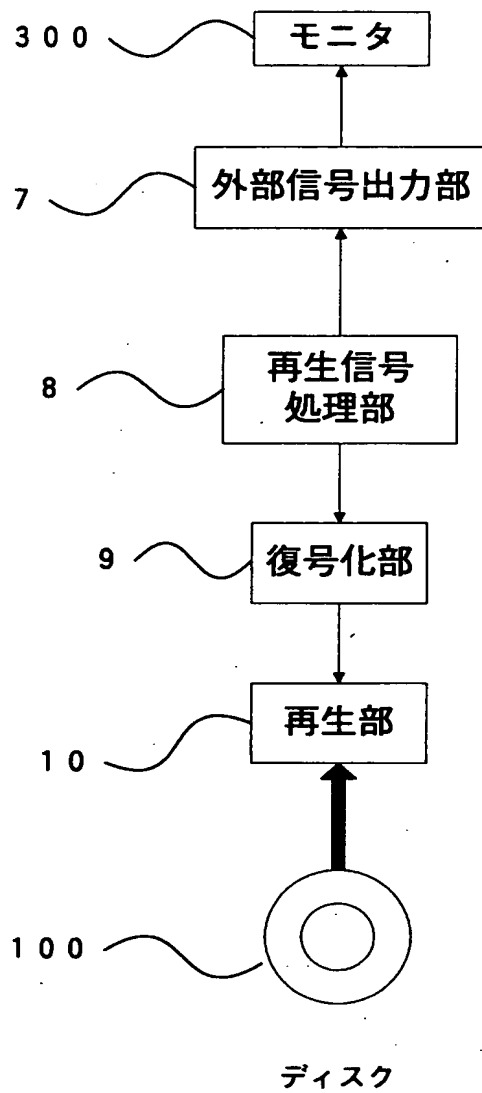
【図 3】



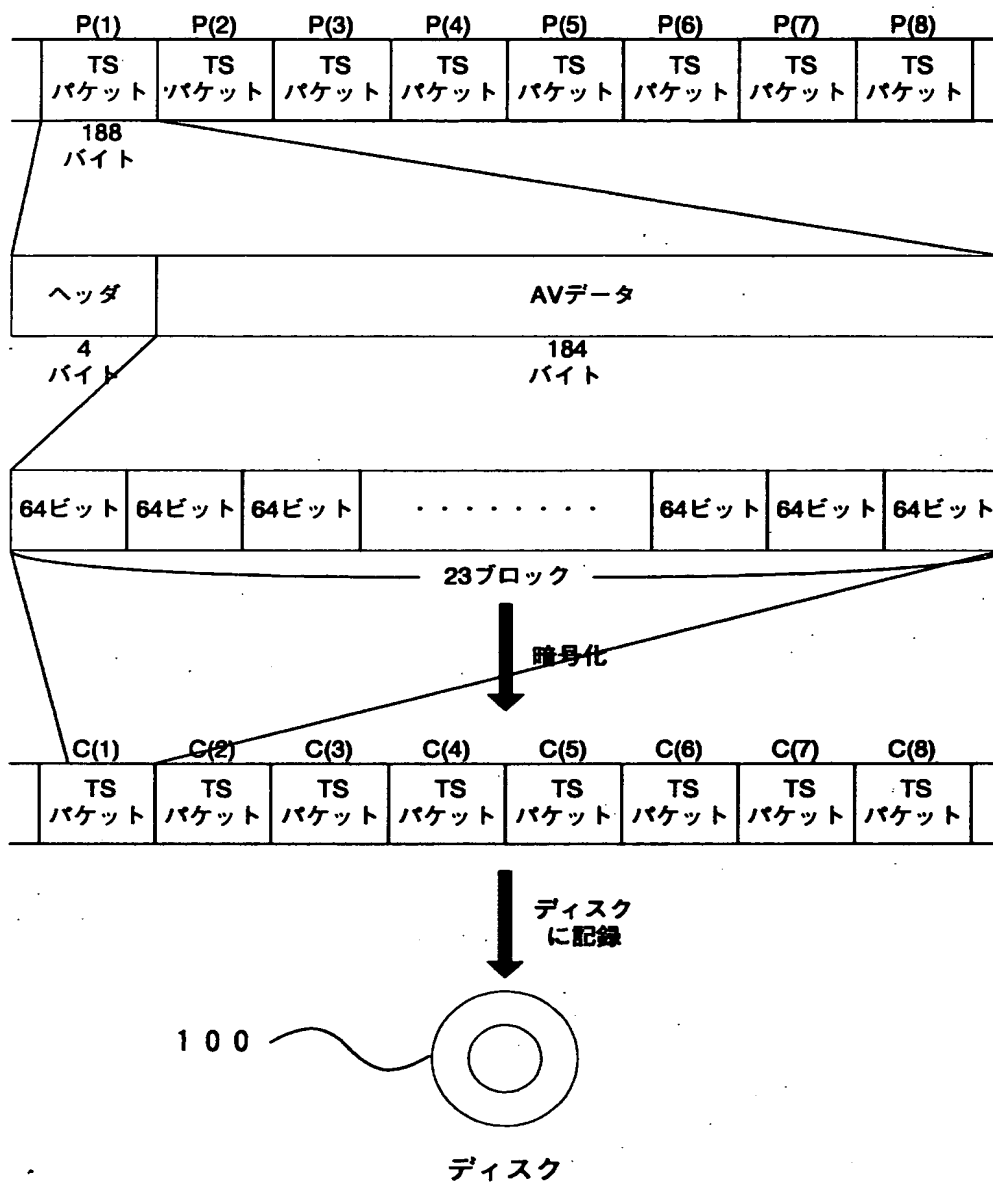
【図 4】



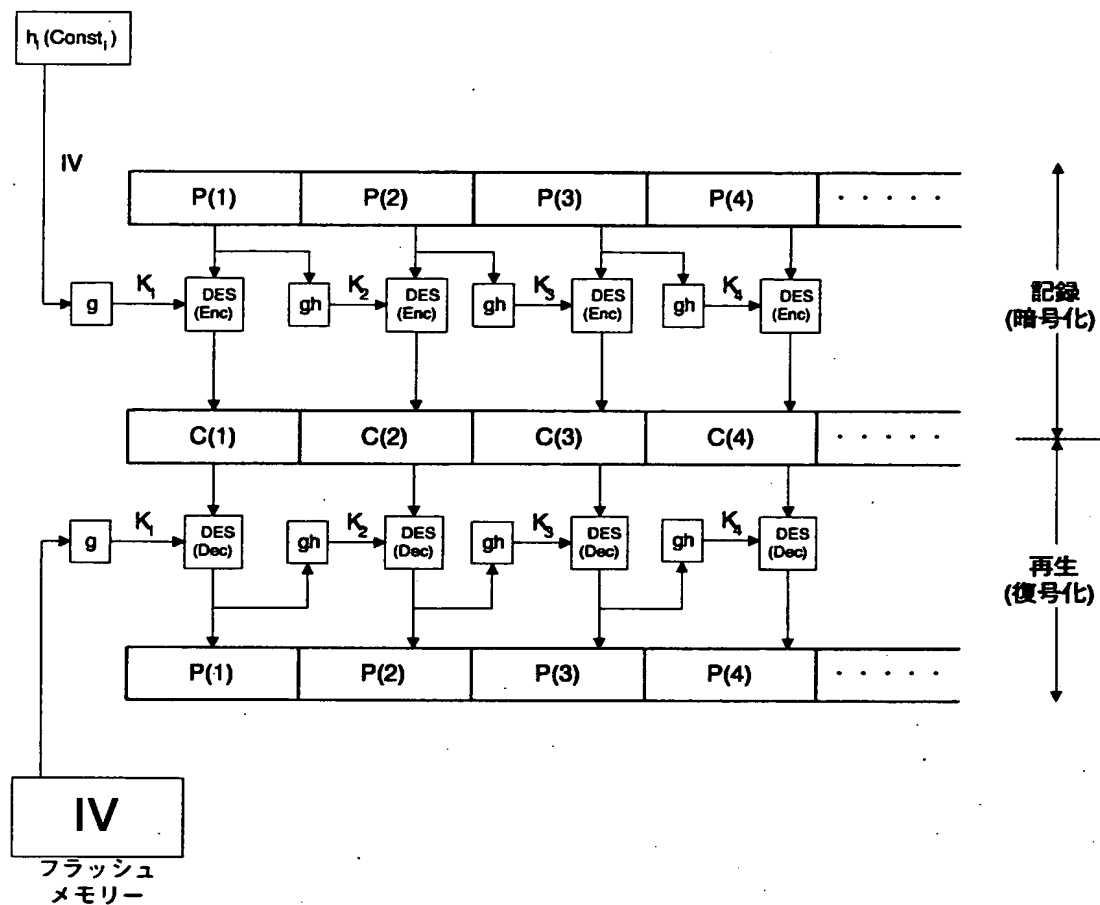
【図 5】



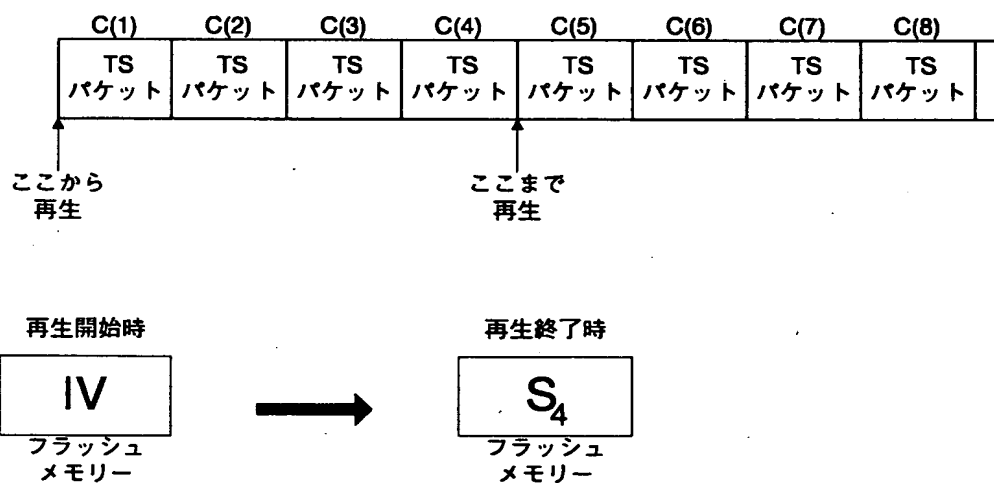
【図 6】



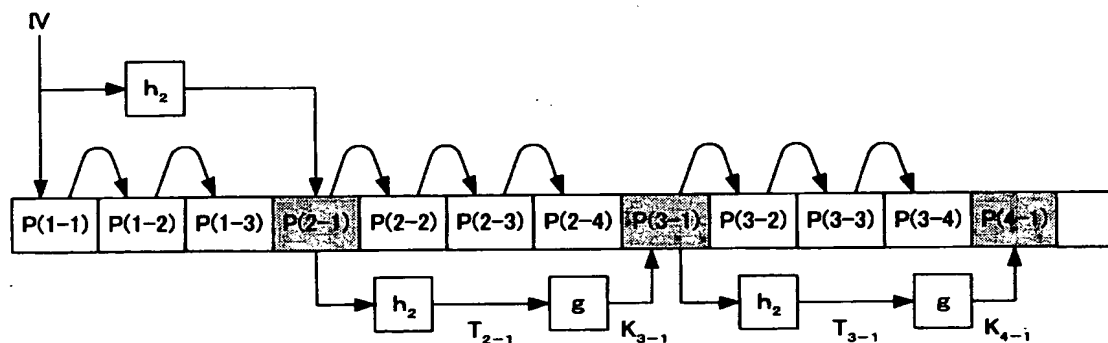
【図 7】



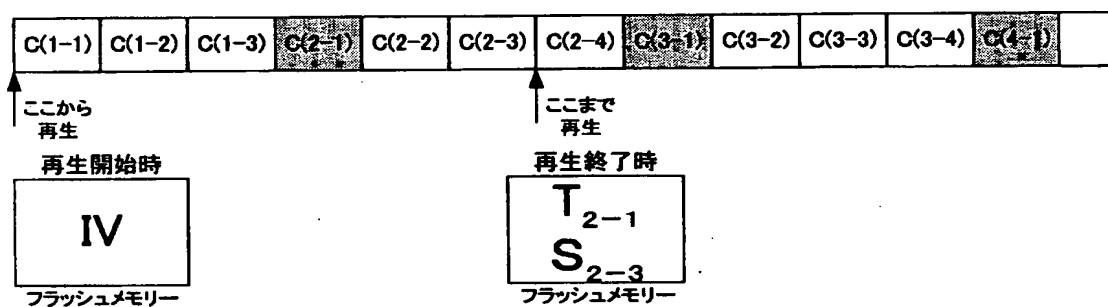
【図 8】



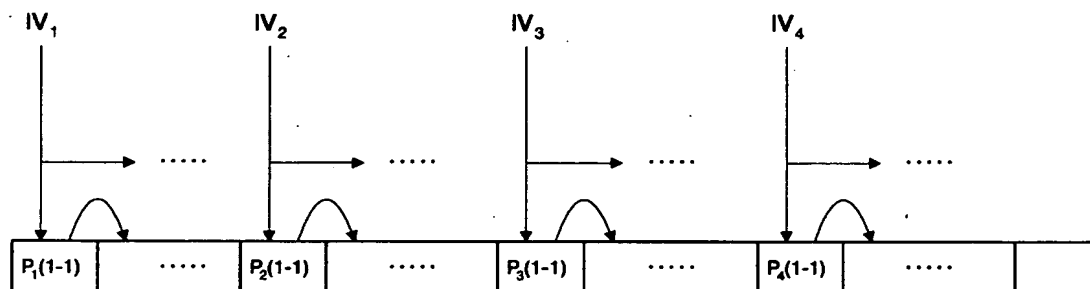
【图9】



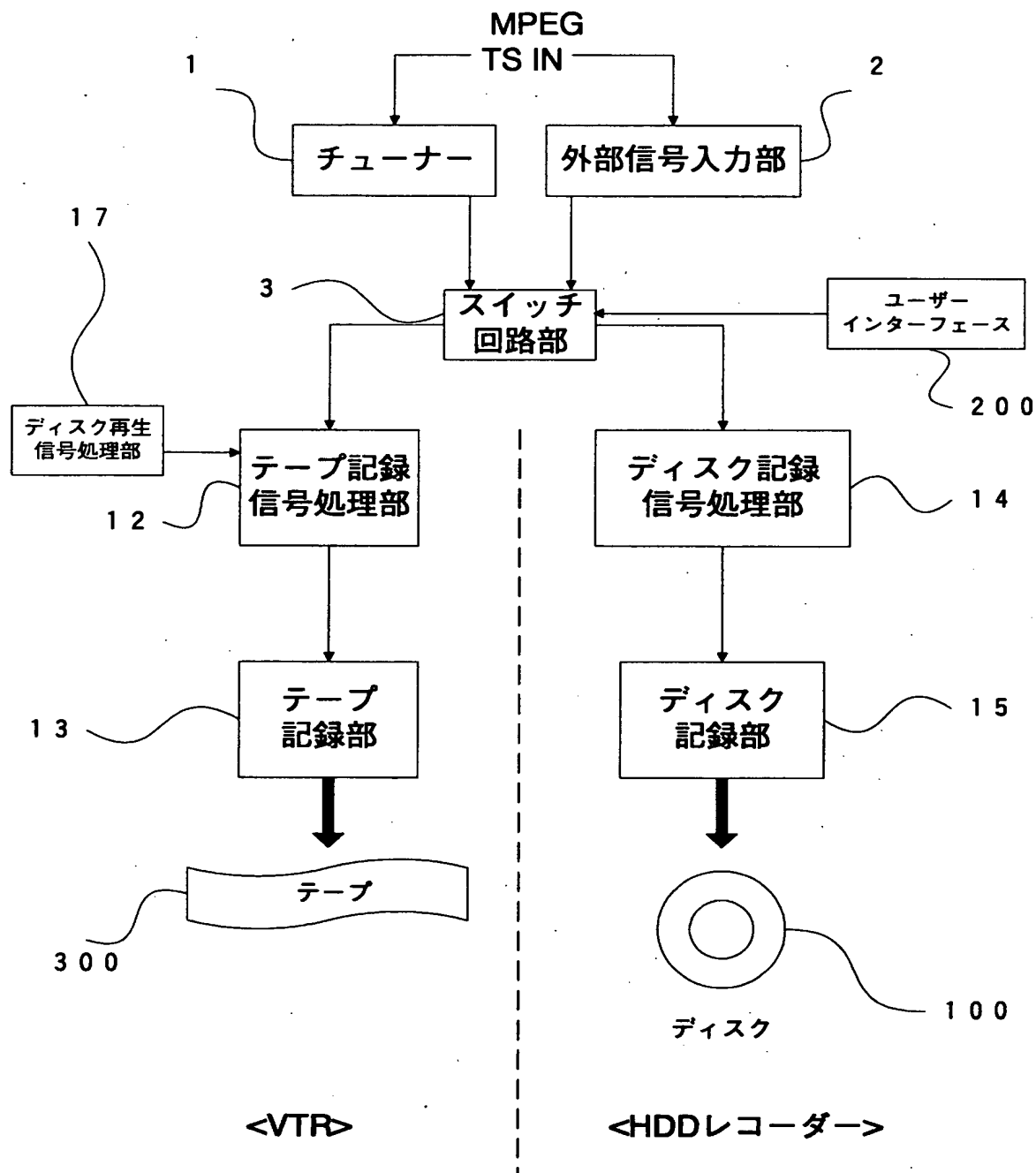
【図 10】



【図 1 1】

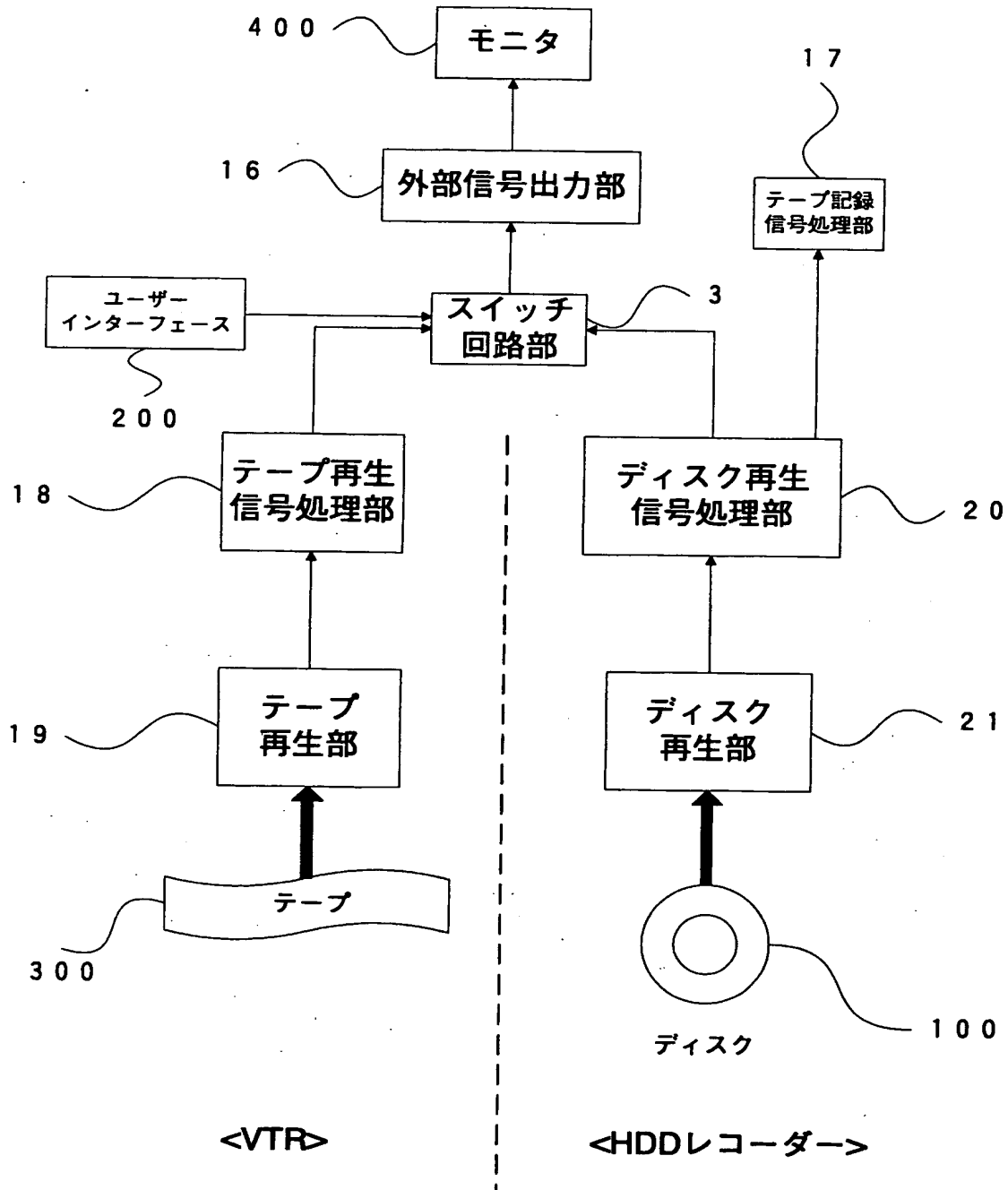


【図 1 2】

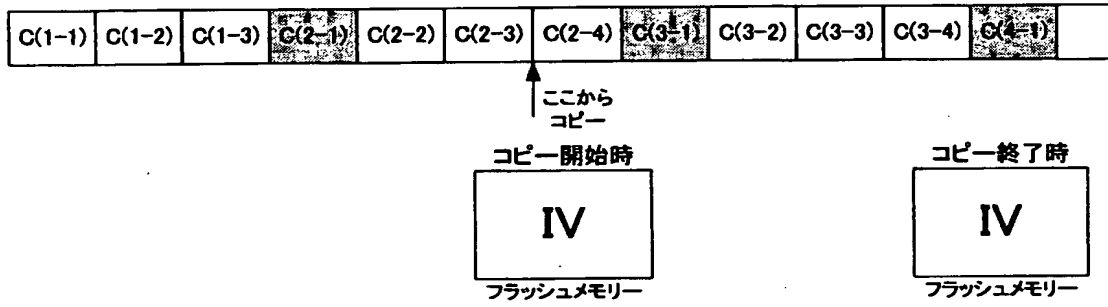




【図13】



【図 1 4】



【書類名】 要約書

【要約】

【課題】 「コピー禁止」のコンテンツについて、視聴者が視聴したい時間にコンテンツを一度のみ視聴することを可能とし、また、「一回コピー可」のコンテンツについて、媒体に記録した後で一度限り別の媒体にコピー及び編集することを可能とすると共に、その際にデータのセキュリティを保障する。

【解決手段】 複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックの暗号文若しくは平文を基にした情報である。

【選択図】 図 7

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日 1990年 8月 8日

[変更理由] 新規登録

住 所 神奈川県横浜市神奈川区守屋町3丁目12番地  
氏 名 日本ビクター株式会社